IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

CONSULTING PROFESSIONAL RESOURCES, INC., Plaintiff	)	
vs	)	CIVIL ACTION NO. 09-1201
CONCISE TECHNOLOGIES LLC, JAMES R. MATTHEWS, and PATRICIA B. ALPHONSE, Defendants	)	

REPORT AND RECOMMENDATION

I. Recommendation

Presently before the court are Defendants, Concise Technologies LLC's ("CT"), James R. Matthews's ("Matthews"), and Patricia B. Alphonse's ("Alphonse"), motions to dismiss the amended complaint under Fed. R. Civ. P. 12(b)(6) for failure to state a claim upon which relief can be granted. It is respectfully recommended that motions to dismiss (Docket Nos. 18 and 20) be granted.

II. Discussion

A. Facts

The plaintiff, Consulting Professional Resources, Inc. ("CPR"), is a Pittsburgh corporation involved in Information Technology ("IT") recruiting and staffing. On behalf of its business clients, CPR recruits candidates in the IT field for

placement in a variety of technical positions and its success is dependent on its ability to attract qualified candidates to accommodate the technical personnel needs of its clients.

On or about July 3, 2002, Matthews was employed by CPR as an Account Manager. When he was hired, Matthews entered into an employment agreement with CPR which provided, inter alia, that:

> The Employee . . . will have access to and become familiar with various trade secrets, consisting of customer lists, compilations of information, and records, which are owned by the Employer and which are regularly used in the operation of the business of the Employer. The Employee shall not disclose any of the aforesaid trade secrets, directly or indirectly, nor use them in any way, either during the term of this Agreement or at any time thereafter, except as required in the course of the Employee's employment.

Pl's Am. Comp. ¶ 14(a). The agreement also restricted Matthews from participating in any business that competed with CPR during his employment and that, upon termination, Matthews was precluded from engaging in competition with CPR for a period of six months and within a fifty-mile radius of the City of Pittsburgh.

While employed with CPR, Matthews was involved in CPR's recruitment functions and had access to information attendant to that responsibility, including CPR's customer lists and contact information, marketing strategies and business plans, information related to qualified IT candidates, as well as other CPR proprietary and confidential information. When Matthews was

promoted to Vice-President in 2003, his responsibilities involved both sales and recruiting, including management of the recruiters. Matthews resigned from CPR on December 22, 2008.

According to the complaint, in October 2008, while still employed by CPR, Matthews formed CT, an entity engaged in the identical IT recruiting and staffing business as CPR. The pleadings further aver that, since October 2008, CT and Matthews have engaged in direct competition with CPR and that some of these competitive activities occurred within a fifty-mile radius of Pittsburgh.

Defendant Alphonse was hired as a recruiter by CPR on or about April 7, 2003 and, in this position, had access to information about CPR's customers, business strategies, finances, and qualified IT candidates. Alphonse also entered into an employment agreement with CPR with limitations on her employment and post-employment activity similar to those agreed upon by Matthews, including the language prohibiting her from " disclos[ing] any of the aforesaid trade secrets, directly or indirectly, nor use them in any way, either during the term of this Agreement or at any time thereafter, except as required in the course of the Employee's employment." Pl's Am. Comp. ¶26 (a).

CPR discovered that as early as January 2009, and until August 2009, while employed at CPR, Alphonse concurrently held

herself out as a "Senior Technical Recruiter" for CT. During this time period, Alphonse allegedly utilized CPR time, resources, and confidential information and disclosed that information to Matthews and CT for the purpose of recruiting qualified IT candidates on behalf of and for the competitive benefit of CT. On or about August 10, 2009, Alphonse's employment with CPR terminated.

On October 26, 2009, CPR filed an amended complaint against CT, Matthews, and Alphonse. In count one, CPR claims that Alphonse violated the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, et seq. ("CFAA"), when she, without authorization, accessed CPR's "protected computer"[1] for the purposes of obtaining and disclosing confidential CPR information to CT and Matthews for the benefit of CT and Matthews. CT's and Matthews's violation of the CFAA allegedly occurred when they obtained CPR's proprietary information from Alphonse. CPR also alleges that it has suffered damage to the integrity of its confidential information by virtue of its transmission to a competitor. CPR additionally claims that it has suffered a cognizable loss under CFAA in excess of $5,000, the amount representing the cost to hire a computer forensic expert to conduct a damage assessment, and attempt to restore CPR's data

[1] As defined by the statute, the term "protected computer" includes a computer "used in or affecting interstate or foreign commerce or communication." 18 U.S.C. § 1030 (e)(2)(B).

and information.

The complaint also includes counts against all defendants for the state law offenses of misappropriation of trade secrets (count two), tortious interference with contractual relations (count three), and conversion (count four). Count five describes a breach of common law duty of loyalty by Matthews and Alphonse. Counts six and seven are against Matthews, alleging breach of fiduciary duty and breach of contract, respectively. Count eight is a breach of contract violation leveled against Alphonse and, finally, count nine outlines a civil conspiracy between Alphonse and Matthews to violate all the above-described offenses. Both Matthews/CT and Alphonse have filed motions to dismiss the amended complaint under Fed. R. Civ. P 12(b)(6).

B. Standard of Review

The United States Supreme Court opinions in Bell Atlantic Corporation v. Twombly, 550 U.S. 544 (2007) and, more recently, in Ashcroft v. Iqbal, 129 S.Ct. 1937 (2009), have shifted pleading standards from simple notice pleading to a more heightened form of pleading, requiring a plaintiff to plead more than the possibility of relief to survive a motion to dismiss.

With the Supreme Court instruction in mind, the Court of Appeals for the Third Circuit has outlined a two-part analysis that courts should utilize when deciding a motion to dismiss for failure

to state a claim. First, the factual and legal elements of a claim should be separated. In other words, while courts must accept all of the complaint's well-pleaded facts as true, they may disregard any legal conclusions. Second, courts then decide whether the facts alleged in the complaint are sufficient to demonstrate that the plaintiff has a "plausible claim for relief." Iqbal, 129 S. Ct. at 1950. That is, a complaint must do more than allege the entitlement to relief, its facts must show such an entitlement. Fowler v. UPMC Shadyside, 578 F.3d 203, 210-211 (3d Cir. 2009).

C. Discussion

1. Computer Fraud and Abuse Act ("CFAA")

The CFAA defines seven actions that can give rise to civil and criminal liability. 18 U.S.C. § 1030 (a) 1-7. In addition to proof that one has committed one of the proscribed activities, civil liability requires an additional showing. Under 18 U.S.C. §1030 (g):

> Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in subclauses (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(I). Damages for a violation involving only conduct described in subsection (c)(4)(A)(i)(I) are limited to economic damages. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery

> of the damage. No action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware.

In other words, a violation of the offenses described in subsection (a) gives rise to civil liability under subsection (g) only if the alleged conduct violates one of the factors set forth in subclauses (I),(II),(III),(IV), or (V) of subsection (c)(4)(A)(i)as follows:

> **(c)** The punishment for an offense under subsection (a) or (b) of this section is-
>
> * * *
>
> **(4)(A)** except as provided in subparagraphs (E) and (F), a fine under this title, imprisonment for not more than 5 years, or both, in the case of--
>
> **(I)** an offense under subsection (a)(5)(B), which does not occur after a conviction for another offense under this section, if the offense caused (or, in the case of an attempted offense, would, if completed, have caused)--
>
> **(I)** loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;
>
> **(II)** the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;
>
> **(III)** physical injury to any person;
>
> **(IV)** a threat to public health or safety;
>
> **(V)** damage affecting a computer used by or for an entity of the United States Government in furtherance of the

> administration of justice, national defense, or national security; or
>
> **(VI)** damage affecting 10 or more protected computers during any 1-year period.

In this matter, CPR claims that Matthews/CT and Alphonse accessed protected CPR computers without authorization or in excess of their authorization in violation of 18 U.S.C. § 1030 (a)(2)(C), knowingly caused the transmission of information, and "as a result of such conduct, intentionally caus[ed] damage without authorization" to CPR computers, in violation of 18 U.S.C. § 1030(a)(5)(A), intentionally accessed CPR computers without authorization and recklessly causing damage as a result, in violation of 18 U.S.C. § 1030(a)(5)(B), and intentionally accessing CPR computers without authorization causing damage and loss, in violation of 18 U.S.C. § 1030(a)(5)(C). CPR further avers that as a result of the defendants' violations of these paragraphs of the CFAA, CPR suffered a loss during a period of one year aggregating at least $5,000, thus giving rise to civil liability under sections 1030(g)and 1030(c)(4)(A)(i)(I).

2. Alphonse's Motion to Dismiss

a. "Without authorization" and "exceeds authorized access"

Alphonse first argues that she cannot be held liable under any provision of the CFAA wherein the alleged violation requires that use of the computer was without authorization or exceeded her authorization, i.e., §§ 1030(a)(2)(C), 1030(a)(5)(B),

1030(a)(5)(C). Alphonse claims that she did not access CPR's computer without authorization nor did she exceed her authorized access of the computer because the activity occurred during the term of her employment when she had permission to utilize CPR computers and to access the information stored therein.

Under the CFAA, one "exceeds authorized access" when he or she "access[es] a computer with authorization and . . . use[s] such access to obtain or alter information in the computer that the accesser is not entitled to obtain or so alter." 18 U.S.C. § 1030(e) (6). The CFAA, however, does not define the term "authorization," and, as a result, two distinct legal theories on the term's meaning have emerged.

The Courts of Appeals in the First and Seventh Circuits, and a number of district courts have concluded that if an employee, although technically authorized to utilize an employers's protected computer, accesses confidential or proprietary information and uses that information in a manner inconsistent with the employer's interests or in a manner that violates a contractual obligation, that employee has exceeded his or her authorized use. See EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577 (1st Cir. 2007); International Airport Centers, LLC v. Citrin, 440 F.3d 418 (7th Cir. 2006); Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc., 119 F.Supp. 2d 1121 (W.D. Wash. 2000). In EF, a former employee provided the defendant/competitor with proprietary

information in order to "mine" his former employer's website for pricing information. In ascertaining whether the defendant's access violated the CFAA, the First Circuit observed that the meaning of "without authorization" was "elusive," id. at 582, n.10., and proceeded to decided the case on whether the defendant exceeded his authorized access. The appeals court found that EF would likely prove that the employee's access exceeded his authorization based upon his confidentiality agreement with EF prohibiting the employee from disclosing any information which could be construed to be contrary to the interests of EF.

This broad reading of "without authorization" was also endorsed by the courts in Citrin and Shurgard, id. In these cases, the courts employed concepts of agency law and concluded that an employee's authority, in regards to access of an employer's computers, "terminates when he acquires adverse interests or is otherwise guilty of a serious breach of loyalty to the principal." Citrin, 440 F.3d at 420-21 (holding that the former employee's breach of loyalty terminated his agency relationship); Shurgard, 119 F.Supp.2d at 1125 (citing Restatement (Second) of Agency § 112 (1958) for proposition that employee's authority ended when he became agent for new employer). Thus, under this school of thought, if an employee breaches the duty of loyalty to an employer, the employee's authorization to access the employer's computer terminates and any subsequent access can give rise to CFAA

liability.

Other courts, however, have rejected reliance on agency law in analyzing the authorization provisions in the CFAA and instead conclude that the statute was enacted to penalize the unauthorized procurement or alteration of information rather than its misuse. In LVRC Holdings LLC v. Brekka, 581 F.3d 1127 (9th Cir.2009), the Court of Appeals for the Ninth Circuit opined that, under a plain-language reading of the statute, "without authorization" means "without permission." Id. at 1133. The court found that no language in the CFAA supports a reading that an employee's authorization terminates when he uses the computer contrary to the employer's interest and offered an interpretation of §§ 1030(a)(2) and (4) which gives effect to both the "without authorization" and "exceeds authorized access" phrases: "a person who 'intentionally accesses a computer without authorization,' §§ 1030(a)(2) and (4), accesses a computer without any permission at all, while a person who 'exceeds authorized access,' id., has permission to access the computer, but accesses information on the computer that the person is not entitled to access." 581 F.3d at 1133. The court concluded that if an employee accesses information from a computer within his permissible parameters, regardless of his subsequent disloyal treatment of that information, he is neither accessing the computer without authorization nor exceeding his authorized access and, therefore, does not violate §§

1030(a)(2) or (a)(4) of the statute. Id. at 1135.

Some district courts who have examined the legislative history of the CFAA find that it supports a narrow reading of the Act. In International Association of Machinists & Aerospace Workers v. Werner-Masuda, 390 F. Supp. 2d 479 (D. Md. 2005), the court observed that the statute was enacted to create a cause of action against "hackers," rather than disloyal employees. Id. at 495 (citing S. Rep. No. 101-544, at 4-5 (1990)(private right of action added to CFAA to combat transmission of viruses and worms)). See also Condux International, Inc. V. Haugum, Civ. No. 08-4824, 2008 WL 5244818, at * 5 (D.Minn. December 15, 2008)(if Congress intended to target person's use of information, it would have provided language to that effect); Shamrock Foods Co. v. Gast, 535 F.Supp. 2d 962, 965 (D.Ariz. 2008)(legislative history of CFAA supports a narrow reading).

Courts advocating a narrow reading of the statute have concluded that the CFAA does not "prohibit the unauthorized disclosure or use of information, but rather unauthorized access. Nor do [its] terms proscribe authorized access for unauthorized or illegitimate purposes." Werner-Masuda, 390 F.Supp. 2d at 499; See also Bridal Expo, Inc. v. Van Florenstein, Civil Action No. 4:08-CV-03777, 2009 WL 255862, at *10 (S.D. Tex. Feb. 3, 2009)(court declining to read CFAA to equate authorization with a duty of loyalty to employer); Lasco Foods, Inc. v. Hall & Shaw Sales,

Marketing, and Consulting LLC, 600 F. Supp. 2d 1045, 1053(E.D. Mo. 2009)(departing employees' misappropriation of information stored on computer was not without authorization as required for CFAA claim where employer permitted employees unrestricted access to its computers); U.S. Bioservices Corporation v. Lugo, 595 F. Supp. 2d 1189, 1192 (D. Kan. 2009)(under CFAA, access to a computer is "without authorization" only when initial access is not permitted and "exceeds authorized access" only when access of certain information is not permitted)); Shamrock Foods 535 F. Supp. 2d at 965 (plain language of CFAA disallows unauthorized procurement or alteration of information, not its misuse); Condux International, 2008 WL 5244818, at *5(same).

The Court of Appeals for the Third Circuit has not taken a position on the "unauthorized access" debate, but it has recognized the trend among employers to employ the "CFAA's civil remedies to sue former employees and their new companies who seek a competitive edge through wrongful use of information from the former employer's computer system." P.C. Yonkers, Inc. v. Celebrations the Party and Seasonal Superstore, LLC., 428 F.3d 504, 510 (3d Cir. 2005). The district courts throughout the Third Circuit, however, have grappled with the issue and have reached divergent results. In Dudick, ex rel. Susquehanna Precision, Inc. v. Vaccarro, Civil Action No. 3:06-CV-2175, 2007 WL 1847435, at * 5 (M.D.Pa. June 25, 2007), the court concluded that an employer

had stated a claim under the CFAA when its employee accessed the employer's proprietary information and used it to benefit a new employer. See also Hub Group, Inc. v. Clancy, No. Civ. A. 05-2046, 2006 WL 208684, at * 4 (E.D. Pa. January 25, 2006)(following Shurgard line of cases and holding that employee's breach of confidentiality agreement equated to CFAA violation).

However, another district court in the Eastern District of Pennsylvania and a district court in this jurisdiction have reached contrary results. In Brett Senior & Associates, P.C. v. Fitzgerald, Civil Action No. 06-1412, 2007 WL 2043377 (E.D. Pa. July 13, 2007), an employer filed an action against a former employee alleging, inter alia, that he had violated a confidentiality agreement when he accessed the employer's computer system to transfer confidential files to a competing firm. The court rejected the employer's position that the employee's access of the computer was unauthorized or exceeded authorized access because he eventually used the information in an improper manner and concluded instead that the lawfulness of the employee's entry into the computer system defeated the progress of the CFAA claim against him. Id. at * 3.

The court in B&B Microscopes v. Armogida, 532 F. Supp. 2d 744 (W.D. Pa. 2007) reached a similar conclusion. Therein , the court rejected the employer's contention that the defendant's conduct in accessing a company laptop violated the CFAA, and

denounced the persuasiveness of those cases holding that an employee's authorized access to a computer is withdrawn if that access is construed as a breach of duty of loyalty to the employer. Id. at 758.

This court likewise declines to construe the CFAA by reliance upon agency principles where the defendant's intent governs whether the access was without authorization or exceeded authorized access. As stated in Brett Senior, cases which focus on the employee's motive for accessing a computer or his eventual use of the information obtained misunderstand the statute to read "'exceeds authorized use' instead of 'exceeds authorized access.'" Here, CPR admits that Alphonse "had access to the confidential trade secret information of CPR . . . ." Pl's Am. Compl. ¶ 27. CPR, therefore, does not allege that Alphonse accessed its computer without authorization or that her access exceeded her authorized access, rather it argues that Alphonse's eventual use of the information accessed violated her employment contract. While disloyal employee conduct might have a remedy in state law, the reach of the CFAA does not extend to instances where the employee was authorized to access the information he later utilized to the possible detriment of his former employer. For this reason, CPR has not stated a claim for which relief can be granted under 18 U.S.C. §§ 1030(a)(2)(C), 1030(a)(5)(B), or 1030(a)(5)(C), as liability under these subsections requires that access was "without

authorization" or "exceed[ed] authorized access."

b. "Damage" under 18 U.S.C. § 1030(a)(5)(A)

It remains to be decided if CPR has adequately pled a violation of subsection 1030(a)(5)(A) which occurs when a person "knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization to a protected computer." As opposed to violations of 18 U.S.C. §§ 1030(a)(2)(C), 1030(a)(5)(B), or 1030(a)(5)(C), a violation of (a)(5)(A) is not determined by unauthorized access, rather, it is predicated on unauthorized damage. In re America Online, Inc., 168 F.Supp.2d 1359, 1371 (S.D.Fla. 2001)(legislative history indicates that subsection(a)(5)(A) covers anyone who damages a computer regardless of whether they were authorized to access the computer).

The CFAA defines "damage" as "any impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. §1030(e)(8). In its amended complaint, CPR described the damage suffered as follows: "the integrity of the proprietary and trade secret data and information on CPR's protected computer has been impaired because its confidentiality and competitive value has been destroyed by its transmission to and use by its direct competitor, [CT]." Pl.'s Am. Comp. ¶60. Alphonse disputes that this is the type of impairment to the integrity of data or information contemplated by the CFAA's

definition of damage.

Given the above-described conflict on the interpretation of "without authorization" and "exceeds authorized access," one can surmise that what constitutes "damage" under the CFAA falls victim to similar debate. Courts advocating a broad interpretation of the Act have concluded that the access and disclosure of trade secrets can constitute an impairment to the integrity of data or information. Shurgard, 119 F.Supp.2d at 1126. See also George S. May International Co. v. Hostetler, No. 04 C 1606, 2004 WL 1197395, at * 4 (N.D.Ill. May 28, 2004)(infringement of copyrighted material taken from protected computer system qualifies as impairment of integrity of copyrighted information).

The other jurisprudential camp disagrees and concludes that misuse of confidential information retrieved from a company's computers does not impair the integrity or availability of data or information. In Garelli Wong & Associates, Inc. v. Nichols,551 F. Supp. 2d 704 (N.D.Ill. January 16, 2008), an employee of a placement agency for accountants who had signed a non-disclosure agreement copied certain confidential information before he left the company. In concluding that CFAA liability does not arise merely by copying data, the court, relying upon and quoting from ResDev, LLC. v. Lot Builders Association Inc., No. 6:04-CV-1374, 2005 WL 1924743, at * 5 n.3 (M.D. Fla. Aug. 10, 2005), decided "that the CFAA's use of word 'integrity' to define damage required

'some diminution in the completeness or usability of data or information on a computer system.'" 551 F. Supp. 2d. at 709. See also Condux, 2008 WL 5244818, at *8 (absent allegations that employee diminished useability of computer information obtained, no CFAA damage occurred, even if employee's activities compromised confidentiality of proprietary information accessed).

Again, this court aligns itself with the courts favoring a narrow reading of the liability provisions of the CFAA. To understand the word "damage" to include inappropriate use of data after it has been accessed lends credence to an interpretation of the CFAA which imposes sanctions for those using computers with authorization and within their authorized access, a construction of the statute which this court has already rejected. If Alphonse had deleted files as did the employee in B & B Microscopes, this activity could give rise to a CFAA cause of action under §1030(a)(5)(A), however, the compromise or decrease in the competitive value of CPR's confidential information does not satisfy the damage requirement of §1030(a)(5)(A).

Because CPR's ability to pursue a CFAA civil claim is dependent upon proof of a substantive violation, CPR's failure to state a cognizable claim under the CFAA requires dismissal of its federal action against Alphonse.

3. Matthews's and CT's Motion to Dismiss

Without statutory citation, CPR's amended complaint alleges that "[i]n obtaining CPR's proprietary and trade secret information through Alphonse as their agent, Matthews/[CT] engaged in the unauthorized access of CPR's computer." Pl.'s Am. Comp. ¶54. The complaint then proceeds to describe Matthews's and CT's liability as contingent upon whether Alphonse's access of CRR's computers was without authorization or exceeded authorized access or whether Alphonse's activity caused damage to a CPR computer. Since it has been decided that CPR has failed to allege sufficient facts that Alphonse violated the CFAA, there can be no liability under the Act for Matthews and CT.

4. State Law Claims

The jurisdictional basis for counts two through nine of the amended complaint is the court's right to exercise supplemental jurisdiction over claims that are a part of the same case or controversy. 28 U.S.C. § 1367(a). It is within the court's discretion to decline to exercise its supplemental jurisdiction over the remaining state law claims. 28 U.S.C. §1367 (c). Having dismissed the count one CFAA claim, the only count within this court's original jurisdiction, the court should decline to exercise supplemental jurisdiction over CPR's state law claims and should dismiss those claims without prejudice.

D. Conclusion

For the reasons stated, the court recommends that Alphonse's and Matthews's and CT's 's motions to dismiss (Docket Nos. 18 and 20) be granted. Within the time limits set forth in the attached notice of electronic filing, any party may serve and file written objections to the Report and Recommendation. Any party opposing the objections shall have fourteen (14) days from the date of service of the objections to respond thereto. Failure to file timely objections may constitute waiver of any appellate rights.

Respectfully submitted,

s/Robert C. Mitchell
Robert C. Mitchell
United States Magistrate Judge

Entered: March 9, 2010